

## Introduction

หลักสูตรนี้เราจะแนะนำการเขียนโปรแกรมที่ถูกหลักการ  
เน้นที่วิธีการเขียนที่สามารถใช้กับภาษาใดๆก็ได้  
หลังจากจบหลักสูตรนี้คุณจะสามารถเข้าใจปัญหาที่เกิดขึ้นกับ Web Application  
โดยส่วนใหญ่รวมทั้งวิธีการป้องกันที่ถูกต้อง รวมทั้งปัญหาที่เกิดขึ้นกับการเขียน Javascript  
ที่ไม่ถูกต้อง

## Course Objective

- เข้าใจวิธีการเขียนโปรแกรมที่ถูกต้อง
- รู้จักการเลือกวิธีการเข้ารหัสที่ถูกต้อง
- เขียน JavaScript ได้ถูกหลักการมากขึ้น
- เลือกวิธีการป้องกันปัญหาได้อย่างถูกต้องมากขึ้น
- รู้จักการ Logging และ Monitoring Application

## Target Group

- Software Developer
- Software Engineer

## Course Outline

### Day 1

1. Security Concept
  - a. OWASP Top 10
  - b. OWASP Proactive Controls

- c. OWASP ASVS
  - d. OWASP Testing Guide
  - e. OWASP Security Principles
- 
- 2. Cross-Origin Resource Sharing (CORS)
    - a. How to CORS work
    - b. Enable CORS
    - c. Add CORS middleware
  - 3. Secure Headers project
    - a. Strict Transport Security (HSTS)
    - b. Content Security Policy (CSP)
    - c. HTTP Public Key Pinning (HPKP)
    - d. X-XSS Protection

## Day 2

- 4. Cryptography
  - a. Offuscation (Encoding)
  - b. Hashing
  - c. Encryption
- 5. Input validation
  - a. Client side vs Server side Validation
  - b. Whitelisting Concept
  - c. Regular Expression
  - d. Validating vs Sanitizing

### Day 3

#### 6. Authentication with JWT

- a. REST API Authentication options
- b. What is JSON Web Token (JWT)
- c. Generating JWTs
- d. Validating JWTs
- e. Using Claims
- f. Authorizing with Claims
- g. JWT attack vectors

#### 7. Exception and Error Handling

- a. Custom error pages
- b. Classify and handling exceptions
- c. Define security policy with Exceptions
- d. Testing error handling

#### 8. Monitoring and Logging application

- a. Elasticsearch
- b. Logstash
- c. Kibana
- d. Beats

Official Training Partner

